EXHIBIT 16

NEWS

KENNESAW STATE UNIVERSITY

Contact: Tammy DeMel, 470/578-6383, tdemel@kennesaw.edu

Kennesaw State statement regarding the Center for Election Systems

KENNESAW, Ga (Mar. 31, 2017) –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was misused following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

###

NEWS

KENNESAW STATE UNIVERSITY

Contact: Tammy DeMel, 470/578-6383, tdemel@kennesaw.edu

Kennesaw State statement regarding the Center for Election Systems

KENNESAW, Ga (Mar. 31, 2017) – Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said Kennesaw State President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

eleted: KSU

###

NEWS

KENNESAW STATE UNIVERSITY

Contact: Tammy DeMel, 470/578-6383, tdemel@kennesaw.edu

Kennesaw State statement regarding the Center for Election Systems

KENNESAW, Ga (Mar. 31, 2017) – Based on a briefing by the Federal Bureau of Investigations (FBI), Kennesaw State officials report that there is no indication of any illegal activity and no personal information was misused following unauthorized access of a dedicated server at the Center for Election Systems.

University officials were first notified of the situation on Wednesday, March 1st and immediately isolated the server and contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We have already begun conversations with experts within the University System of Georgia and an outside firm to validate that university systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

###

NEWS

KENNESAW STATE UNIVERSITY

Contact: Tammy DeMel, 470/578-6383, tdemel@kennesaw.edu

Kennesaw State statement regarding the Center for Election Systems

KENNESAW, Ga (Mar. 31, 2017) –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

“We are working with experts within the University System of Georgia and an outside firm to validate that KSU’s systems are secured and meet best practice standards,” said KSU President Sam Olens. “We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney’s Office in helping us resolve this issue.”

###

NEWS

KENNESAW STATE UNIVERSITY

Contact: Tammy DeMel, 470/578-6383, tdemel@kennesaw.edu

Kennesaw State statement regarding the Center for Election Systems

KENNESAW, Ga (Mar. 31, 2017) –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was misused following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

###

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

> **KENNESAW, Ga (Mar. 31, 2017)** –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).
>
> University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.
>
> "We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately $2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)
Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.
Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.
Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.
Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.
Action Item Owner: UITS-ISO. KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the [redacted] (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.
Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.
    1. Rackmount UPS Battery backups (one displaying warning light)
    Recommendation: Replace batteries as needed and move under UITS ISS management
    2. 3com Switches – Age 10+ years -- No Support -- L2 only
    Recommendation: Replace and move under UITS ISS management
    3. Dell 1950 (Windows Domain Controller) – Age 10+ years
    Recommendation: Surplus
    4. Dell PowerEdge R630 – Age 1 year
    Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
    5. EPIC – Vision Computer – Age Unknown – Ballot creation box
    Recommendation: Continue as ISO/CES managed
    6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups
    Recommendation: Surplus
    7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
    Recommendation: Surplus
    8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950

Recommendation: Surplus

10. Web server backup

Recommendation: Surplus

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

8. Issue: An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

9. Issue: A wireless access point was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.

Action Item Owner: UITS-ISO, UITS-ISS

10. Issue: Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone
Green = KSU data public network
Blue = Elections private network
White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately $3,000.

Action Item Owner: UITS-ISO, UITS-ISS

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

> **KENNESAW, Ga (Mar. 31, 2017)** –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).
>
> University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.
>
> "We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately $2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)
Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server were running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited to the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.
Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were defined, but not documented.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.
Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff were not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.
Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** The door to Room 105b, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.
Action Item Owner: UITS-ISO. KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the [redacted] (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.
Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.
    1. Rackmount UPS Battery backups (one displaying warning light)
    Recommendation: Replace batteries as needed and move under UITS ISS management
    2. 3com Switches – Age 10+ years -- No Support -- L2 only
    Recommendation: Replace and move under UITS ISS management
    3. Dell 1950 (Windows Domain Controller) – Age 10+ years
    Recommendation: Surplus
    4. Dell PowerEdge R630 – Age 1 year
    Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
    5. EPIC – Vision Computer – Age Unknown – Electors List creation box
    Recommendation: Continue as ISO/CES managed
    6. EPIC Files – Dell 1900 – Age 6+ years – Electors List backups
    Recommendation: Surplus
    7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
    Recommendation: Surplus
    8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950

Recommendation: Surplus

10. Web server backup

Recommendation: Surplus

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

8. Issue: An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

9. Issue: A wireless access point managed by CES Staff was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.

Action Item Owner: UITS-ISO, UITS-ISS

10. Issue: Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone
Green = KSU data public network
Blue = Elections private network
White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105b, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately $3,000.

Action Item Owner: UITS-ISO, UITS-ISS

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

> **KENNESAW, Ga (Mar. 31, 2017) –**Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).
>
> University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.
>
> "We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately $2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)
Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server were running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited to the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.
Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were defined, but not documented.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.
Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff were not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.
Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** The door to Room 105b, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.
Action Item Owner: UITS-ISO. KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the [redacted] – (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.
Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.

    1. Rackmount UPS Battery backups (one displaying warning light)
    Recommendation: Replace batteries as needed and move under UITS ISS management
    2. 3com Switches – Age 10+ years -- No Support -- L2 only
    Recommendation: Replace and move under UITS ISS management
    3. Dell 1950 (Windows Domain Controller) – Age 10+ years
    Recommendation: Surplus
    4. Dell PowerEdge R630 – Age 1 year
    Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
    5. EPIC – Vision Computer – Age Unknown – Electors List creation box
    Recommendation: Continue as ISO/CES managed
    6. EPIC Files – Dell 1900 – Age 6+ years – Electors List backups
    Recommendation: Surplus
    7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
    Recommendation: Surplus

8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610
Recommendation: Format and reinstall on CES Isolated Network as NAS
9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950
Recommendation: Surplus
10. Web server backup
Recommendation: Surplus

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

8. **Issue:** An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

9. **Issue:** A wireless access point managed by CES Staff was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.

Action Item Owner: UITS-ISO, UITS-ISS

10. **Issue:** Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone
Green = KSU data public network
Blue = Elections private network
White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105b, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately $3,000.

Action Item Owner: UITS-ISO, UITS-ISS

From: Stephen Gay
To: Stephen Gay
Subject: FW: Incident Reponse Walk through
Date: Thursday, October 26, 2017 4:19:53 PM
Attachments: CES AAR - MBedits 042617.docx

-----Original Message-----
From: Michael Barnes
Sent: Wednesday, April 26, 2017 3:30 PM
To: Stephen Gay <sgay@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher Dehner <cmd9090@kennesaw.edu>; Merle King <mking@kennesaw.edu>
Subject: RE: Incident Reponse Walk through

Stephen,

Thank you for giving us the opportunity to review the attached. We have provided a few grammatical changes and added just a few clarifying comments.
I am attaching a copy with Change Tracker on so you can quickly see those changes.

We have asked Steven Dean to follow up with Chris Dehner to see what timeline may be in place in relation to items listed in Issue 7. We want to make sure we are doing our part but we will need some guidance.

Please let us know what other assistance we can provide.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Monday, April 24, 2017 12:01 PM
To: Merle King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher M. Dehner <cmd9090@kennesaw.edu>
Subject: Re: Incident Reponse Walk through

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,
Stephen

----- Original Message -----
From: "Merle King" <mking@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>
Sent: Tuesday, April 18, 2017 9:55:05 AM
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SOS IT staff in the exercise.

Thanks in advance,

Merle

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

From: Stephen Gay
To: Stephen Gay
Subject: FW: Incident Reponse Walk through
Date: Thursday, October 26, 2017 4:19:28 PM
Attachments: CES AAR Rev04.pdf

-----Original Message-----
From: Stephen Gay
Sent: Thursday, April 27, 2017 10:29 AM
To: Michael Barnes <mbarne28@kennesaw.edu>; Merle King <mking@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher Dehner <cmd9090@kennesaw.edu>
Subject: Re: Incident Reponse Walk through

Michael and Merle,

Thank you for the edits. I have accepted them and attached the updated version and will be on the lookout for the referenced email.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director Information Security Office University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, April 26, 2017 3:29:43 PM
Subject: RE: Incident Reponse Walk through

Stephen,

Thank you for giving us the opportunity to review the attached. We have provided a few grammatical changes and added just a few clarifying comments.
I am attaching a copy with Change Tracker on so you can quickly see those changes.

We have asked Steven Dean to follow up with Chris Dehner to see what timeline may be in place in relation to items listed in Issue 7. We want to make sure we are doing our part but we will need some guidance.

Please let us know what other assistance we can provide.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road

Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Monday, April 24, 2017 12:01 PM
To: Merle King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher M. Dehner <cmd9090@kennesaw.edu>
Subject: Re: Incident Reponse Walk through

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,
Stephen

----- Original Message -----
From: "Merle King" <mking@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>
Sent: Tuesday, April 18, 2017 9:55:05 AM
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SOS IT staff in the exercise.

Thanks in advance,

Merle

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

From: Stephen Gay
To: Stephen Gay
Subject: FW: Incident Reponse Walk through
Date: Thursday, October 26, 2017 4:19:27 PM
Attachments: CES AAR.docx

-----Original Message-----
From: Stephen Gay
Sent: Monday, April 24, 2017 12:02 PM
To: Merle King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher Dehner <cmd9090@kennesaw.edu>
Subject: Re: Incident Reponse Walk through

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,
Stephen

----- Original Message -----
From: "Merle King" <mking@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>
Sent: Tuesday, April 18, 2017 9:55:05 AM
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SOS IT staff in the exercise.

Thanks in advance,

Merle

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900

Fax: 470-578-9012

Michael Barnes

From: Merle Steven King
Sent: Sunday, August 28, 2016 3:56 PM
To: Steven Jay Dean; Jason Stephen Figueroa
Cc: Michael L. Barnes
Subject: Fwd: [IMPORTANT] concerning the security of elections.kennesaw.edu

Steven and Jason - Please review this email and advise. Sooner is better than later.

Thanks,

MSK

From: "Logan Lamb"
To: "Merle King"
Cc: research@bastille.net
Sent: Sunday, August 28, 2016 3:47:50 PM
Subject: [IMPORTANT] concerning the security of elections.kennesaw.edu

Hello Merle,

My name is Logan Lamb, and I'm a cybersecurity researcher who is a member of Bastille Threat Research Team. We work to secure devices against new and existing wireless threats: https://www.bastille.net/. This past Tuesday I went to Fulton County Government Center to speak with Rick Barron about securing voting machines against wireless threats. I was then directed to contact you and the center. I'd like to collaborate with you on securing our state's election systems infrastructure against wireless attacks.

While attempting to get more background information on the center prior to contacting you, I discovered serious vulnerabilities affecting elections.kennesaw.edu.

The following google searches reveal documents that shouldn't be indexed and appear to be critical to the elections process. In addition, the Drupal install needs to be immediately upgraded from the current version, 7.31:

"site:elections.kennesaw.edu inurl:pdf"
I generally use this type of search to find documents on websites that lack search functionality. This search revealed a completely open Drupal install.

Assume any document that requires authorization has already been downloaded without authorization.

"site:elections.kennesaw.edu L&A"
The second search result appears to be for disseminating critical voting system software. This is especially concerning because, as the following article states, there's a strong probability that your site is already compromised.
https://www.drupal.org/project/drupalgeddon
https://www.drupal.org/SA-CORE-2014-005

If you have any questions or concerns please contact me. I'm able to come to the center this Monday for a more thorough discussion.

Take care,
Logan

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

Michael Barnes

From:	Merle Steven King
Sent:	Wednesday, March 01, 2017 11:45 PM
To:	Michael L. Barnes; Steven Jay Dean
Subject:	Fwd: Vulnerability on the elections.kennesaw.edu website

FYI.

Sent from my iPad

Begin forwarded message:

> **From:** "Stephen C. Gay" <sgay@kennesaw.edu>
> **Date:** March 1, 2017 at 11:10:16 PM EST
> **To:** Merle King <mking@kennesaw.edu>, Steven Dean <sdean29@kennesaw.edu>
> **Cc:** Lectra Lawhorne <llawhorn@kennesaw.edu>, "William C. Moore" <wmoore36@kennesaw.edu>
> **Subject: Fwd: Vulnerability on the elections.kennesaw.edu website**
>
> Merle,
>
> I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.
>
> I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Forwarded Message -----

From: "Andy Green" <agreen57@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Sent: Wednesday, March 1, 2017 9:55:27 PM
Subject: Vulnerability on the elections.kennesaw.edu website

Stephen,

Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.

My friend shared with me that the exposed directories contained, among other things:
- voter registration detail files, including DOB and full SSN.
- PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day access, for the November 2016 election.

I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.

The base URL of interest is http://elections.kennesaw.edu/sites/default/files - please note that the URL must be http, as use of https will return a 404 error.

I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.

If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.

Thanks

Andy Green, MSIS

Lecturer of Information Security and Assurance
BBA-ISA program coordinator
KSU Student ISSA chapter faculty sponsor
KSU Offensive Security Research Club faculty sponsor

Michael J. Coles College of Business
Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
560 Parliament Garden Way NW, MD 0405
Kennesaw, GA 30144-5591

agreen57@kennesaw.edu
http://coles.kennesaw.edu/faculty/green-andrew.php
Ph: 470-578-4352
Burruss Building, Room #490

73656d706572207061726174747573

Michael Barnes

From:	Stephen Craig Gay
Sent:	Thursday, April 27, 2017 10:29 AM
To:	Michael L. Barnes; Merle Steven King
Cc:	Lectra Lawhorne; Christopher Michael Dehner
Subject:	Re: Incident Reponse Walk through
Attachments:	CES AAR Rev04.pdf

Michael and Merle,

Thank you for the edits. I have accepted them and attached the updated version and will be on the lookout for the referenced email.

Stephen C Gay CISSP CISA
KSU Chief Information Security Officer & UITS Executive Director Information Security Office University Information Technology Services (UITS) Kennesaw State University Technology Services Bldg, Room 031
1075 Canton Pl, MB #3503
Kennesaw, GA 30144
Phone: (470) 578-6620
Fax: (470) 578-9050
sgay@kennesaw.edu

----- Original Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "cmd9090" <cmd9090@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, April 26, 2017 3:29:43 PM
Subject: RE: Incident Reponse Walk through

Stephen,

Thank you for giving us the opportunity to review the attached. We have provided a few grammatical changes and added just a few clarifying comments.
I am attaching a copy with Change Tracker on so you can quickly see those changes.

We have asked Steven Dean to follow up with Chris Dehner to see what timeline may be in place in relation to items listed in Issue 7. We want to make sure we are doing our part but we will need some guidance.

Please let us know what other assistance we can provide.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144

ph: 470-KSU-6900
fax: 470-KSU-9012
-----Original Message-----
From: Stephen C. Gay [mailto:sgay@kennesaw.edu]
Sent: Monday, April 24, 2017 12:01 PM
To: Merle King <mking@kennesaw.edu>; Michael Barnes <mbarne28@kennesaw.edu>
Cc: Lectra Lawhorne <llawhorn@kennesaw.edu>; Christopher M. Dehner <cmd9090@kennesaw.edu>
Subject: Re: Incident Reponse Walk through

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,
Stephen

----- Original Message -----
From: "Merle King" <mking@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>
Sent: Tuesday, April 18, 2017 9:55:05 AM
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SOS IT staff in the exercise.

Thanks in advance,

Merle

--
Merle S. King

Executive Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, Georgia 30144

Voice: 470-578-6900
Fax: 470-578-9012

From: Merle Steven King
To: Stephen Craig Gay
Subject: Re: Vulnerability on the elections.kennesaw.edu website
Date: Wednesday, March 1, 2017 11:41:01 PM

Stephen - We will investigate and advise.

Merle

Sent from my iPad

> On Mar 1, 2017, at 11:10 PM, Stephen C. Gay <sgay@kennesaw.edu> wrote:
>
> Merle,
>
> I received the following email, and call, tonight regarding a directory traversal vulnerability on elections.kennesaw.edu. I immediately activated our Incident Response Team and, through the use of burp suite, we were able to recreate the vulnerability described below. In the vulnerability recreation, we were able to pull voter information in database files for counties across the state and the data elements included DOB, Drivers License Number, Party Affiliation, etc. Understanding the risk associated with this vulnerability, we have closed all firewall exceptions for elections.kennesaw.edu to contain the incident. I have asked Bill Moore to act as point for this incident and we need to coordinate with your team on the web logs for elections.kennesaw.edu first thing tomorrow morning. The logs will help us understand the scope of the breach and allow us to advise the CIO as to next steps.
>
> I will be temporarily out of pocket for a short time tomorrow, then remote thereafter, but your cooperation in this incident response is appreciated.
>
> Stephen C Gay CISSP CISA
> KSU Chief Information Security Officer & UITS Executive Director
> Information Security Office
> University Information Technology Services (UITS)
> Kennesaw State University
> Technology Services Bldg, Room 031
> 1075 Canton Pl, MB #3503
> Kennesaw, GA 30144
> Phone: (470) 578-6620
> Fax: (470) 578-9050
> sgay@kennesaw.edu
>
> ----- Forwarded Message -----
> From: "Andy Green" <agreen57@kennesaw.edu>
> To: "Stephen C Gay" <sgay@kennesaw.edu>
> Sent: Wednesday, March 1, 2017 9:55:27 PM
> Subject: Vulnerability on the elections.kennesaw.edu website
>
> Stephen,
>
> Thanks for taking the time to talk with me tonight. As I mentioned during our call, I was contacted by a friend in the security space here in Atlanta earlier tonight. My friend relayed to me the existence of a Drupal plug-in vulnerability that a friend of his located on the elections.kennesaw.edu website. The vulnerability allows for directory traversal without authentication, leaving files exposed.
>
> My friend shared with me that the exposed directories contained, among other things:
> - voter registration detail files, including DOB and full SSN.
> - PDFs of memos to county election officials which contained full credentials for ExpressPoll Election Day

access, for the November 2016 election.
>
> I was able to verify the presence of the vulnerability myself, and was able to traverse directories without authenticating. I did not download any of the voter data files to verify his statement, for obvious reasons. However, I did successfully open a PDF in my browser window, located in the Fulton County Elections/ExpressPoll/ED_Files/ folder for proof of concept.
>
> The base URL of interest is http://elections.kennesaw.edu/sites/default/files - please note that the URL must be http, as use of https will return a 404 error.
>
> I'm told the researcher works for a reputable organization. I'm also told that the organization may be interested in going public with this at some point, due to the seriousness of the matter as well as the related publicity it would generate for the organization. My sense is that there is a desire to go public in a coordinated, responsible manner, in order to give the university appropriate time to remediate the vulnerability. This is certainly not set in bedrock, as I'm just the middleman here. However, given that they reached out to me as opposed to releasing to the public, I'm hopeful that my sense is correct.
>
> If I can be of further service, including facilitating communication between all parties, please don't hesitate to let me know.
>
> Thanks
>
> Andy Green, MSIS
>
> Lecturer of Information Security and Assurance
> BBA-ISA program coordinator
> KSU Student ISSA chapter faculty sponsor
> KSU Offensive Security Research Club faculty sponsor
>
> Michael J. Coles College of Business
> Kennesaw State University - A Center of Academic Excellence in Information Assurance Education
> 560 Parliament Garden Way NW, MD 0405
> Kennesaw, GA 30144-5591
> agreen57@kennesaw.edu
> http://coles.kennesaw.edu/faculty/green-andrew.php
> Ph: 470-578-4352
> Burruss Building, Room #490
>
> 73656d70657220706172617261747573